REMARKS/ARGUMENTS

This Amendment is in response to the Office Action dated December 24, 2003. Claims 1-39 are pending, claims 1-4, 6, 16, 18, 20, 22, 24, 25, 26, and 27-29 have been amended, and claims 40-42 have been added. Claims 1-42 remain pending.

A telephone interviewed between Examiner Ellisca, Joe Fontana, and Stephen Sullivan occurred on February 13, 2003. The substance of the interview is set forth herein.

Independent claims 1, 16, 22, and 24 have been amended to recite that the encryption key used to encrypt the software is "derived from a dynamic key, which is assigned to the software to be protected and does not change between copies of the software." Support for the amendment may be found throughout the specification, see pg. 11, lines 26-28, for example. A portion of the limitations of dependent claims 13-15 has been added to claims 1 and 24 as new step (b), which recites that in response to the security device being coupled to the computer system, information identifying the protected software is sent from the computer system to the security device. Step (c) has been amended to recite that the information supplied from the software is used to determine if the dynamic key assigned to the software is present in the security device, and if so, generating the encryption key within the security device using the dynamic key. Claim 16 has been amended to recite that at least a portion of information sent from the computer to the device "identifies the protected software." The dependent claims have been amended to provide proper antecedent basis. New claims 40-42 have been added to more particularly claim the present invention. Accordingly, no new matter has been entered.

The Examiner rejected claims 1-3, 6-17, 20-22, 24-26, and 29-39 under 35 USC §102(b) as being anticipated by Chou et al. (US Pat. No. 5,222,133). Claims 4, 5, 18, 19, 23, 27, and 28 are objected to but would be allowable if rewritten in independent form.

As discussed during the telephone interview, it is believed that Chou fails to teach or suggest the combination of elements in the amended independent claims. For example, the claims now recite that the dynamic key used to derive the encryption key is assigned to the software to be protected and does not change between copies of the software. Once the security device is coupled to the computer system, information identifying the software is sent to the security device. The security device uses this information to determine whether the matching encryption key is present in the security device (the security device may have multiple such keys related to different software products). Only if the corresponding encryption key is present does the security device generate the encryption key and send the encryption key to the computer system.

Chou fails to teach or suggest any of the above as there are several differences between the claimed invention and Chou's keys and the method Chou uses to authenticate the software. First, the dynamic key of the present invention is assigned to a particular *software product* and used to generate an encryption key to keep the encryption key secret. In Chou, in contrast, the key pair comprising the first and second keys is unique to the *user* (see col. 3, lines 40-45).

In addition, Chou's first key is simply stored in the security device and not "generated". Therefore, Chou does teach or suggest "generating the encryption key within the security device," as recited in claims 1 and 24. In fact, none of Chou's keys (first key, second key or the control key) is analogous to the encryption key, because none of Chou's keys are described to be used for encryption. The control key is probably the closest to being analogous the encryption key, but only because the control key is generated. However, Chou's control key is generated on the computer, while the claimed encryption key is generated on the security device.

One reason Chou simply stores the first key is because Chou specifically states the first key "is not secret" (col. 3, line 49); therefore there is no need to generate it at the time of authentication. From a security standpoint, where one stores and generate keys is very important to the method of protection. If the first key is going to be exposed, the second key, and the algorithm on the computer (the hacker's playground), hacker's have a chance to defeat the security system. In Chou's invention, the control key is like a password, e.g., one has to have the right password to run the program. The security issue with this method is that software that verifies the control key is susceptible to a simple code removal attacks by a hacker. Basically, the gatekeeper that stops the program from running is simply removed.

The claimed invention uses a different method of protection; the generation of the encryption key and even the dynamic key itself are kept secret in the security device to prevent such hacking. Encryption/decryption is a better method of protection, because there is no simple hacker attack. If a hacker removes the code that does the decryption, then the software is still protected by the fact that it remains encrypted.

Not only does Chou fail to teach or suggest that the encryption key is generated within the security device, Chou also fails to teach or suggest "using information supplied from the software to determine if the dynamic key assigned to the software is present in the security device, and if so, generating the encryption key within the security device using the dynamic key," as recited in claims 1 and 24. Independent claims 16, 22, 24, and 39 have similar recitations.

As previously argued, Chou does not teach or suggest the sending any information from the computer system to the security device. Referring to claim 22 as a further example, the security key (encryption key in claim 1) is generated using an initialization vector and the dynamic key. The initialization vector is provided with the software and the dynamic key is stored on the security device. During authentication, the initialization vector is *sent from the computer system to the security device*, where it is used with the dynamic key assigned to the software to generate the encryption key. In contrast, Chou's second key input to the computer system is never sent to the security device. As a result, there is no way to generate Chou's control key on the security device.

In addition, Applicant maintains the arguments presented in the previous amendments. Further, claims 16, 22 and 39 should be independently allowable as they include additional recitations than claims 1 and 24.

New claim 40 is similar to claim 1, but includes recitations regarding a communications key, which, like the encryption key, is also derived by the dynamic key. The communications key is used in the security device to encrypt the encryption key prior to the encryption key being sent to the computer system. As stated above, Chou's first key is not secret; and therefore Chou does not teach encrypting the first key on the security device before sending it to the computer. And even if Chou did teach such encryption, Chou would fail to teach or suggest that the first key was encrypted with a key that was derived from key used to generate the first key (as stated above, Chou does not teach generating the first key).

Therefore, for the above identified reasons, the present invention as recited in claims 1-41 is neither taught nor suggested by Chou. In view of the foregoing, Applicant submits that claims 1-41 are patentable over the cited reference. Applicant, therefore, respectfully requests reconsideration and allowance of the claims as now presented.

Applicants' attorney believes this application in condition for allowance. Should any unresolved issues remain, Examiner is invited to call Applicants' attorney at the telephone number indicated below.

Respectfully submitted,
SAWYER LAW GROUP LLP

March 12, 2004
Date

Stephen Sullivan
Sawyer Law Group LLP
Attorney for Applicant(s)
Reg. No. 38,329
(650) 493-4540

r